EXHIBIT A

J. Richard Kiper, PhD, PMP

FBI Special Agent (Retired) and Forensic Examiner

June 30, 2023

Summary of Findings

I. Professional Background

I served as an FBI Special Agent for 20 years, from 1999 to 2019, with more than half of that career in cybersecurity and digital forensics (See attached CV). In the FBI, I served as a case agent, a supervisor, a unit chief, a forensic examiner, a trainer of forensic examiners, and a trainer of other trainers of forensic examiners. I have personally worked on dozens of child pornography investigations and examined hundreds of pieces of evidence seized from those who have been charged with receipt, possession, and transportation of child pornography. I have an in-depth knowledge of file systems and operating systems, FBI evidence handling procedures, and of digital evidence examination procedures and policies.

II. Review of Evidence

The current case, U.S. v. SCHULTE, involves dozens of computing devices holding multiple terabytes of data, as well as thousands of pages of case documents. My review of materials included, for example, the government's charging documents, forensic copies of seized devices, FD-302 reports documenting interviews, FBI prepossessed evidence views, 11 years of Google searches, four years of IRC chats, file and directory listings, user account information, and specific files contained within seized evidence, such as logs, configuration files, Windows registry hives, and other Windows artifacts of user activity. I note that I did not have access to the computer system from which the child pornography (CP) material was copied to Schulte's computer system seized at the search. For reasons I describe below, I believe the computer was part of a malfunctioning system that had been reformatted and repurposed prior to the 03/15/2017 search.

Due to the nature and extent of evidence, I was limited in my access and review of the digital evidence in this case.[1] However, I am confident of the findings I present in this report based on

[1] The FBI was very accommodating to my review of evidence under their supervision. However, at the time of this writing, I have not yet received several items I requested from the government, including file listings of certain virtual machines, a listing of file and folder permissions of two seized devices, and a documented accounting (redacted if necessary) of FBI activity during the 03/15/2017 search of Schulte's residence, which resulted in the changing of filesystem timestamps of hundreds of files located on the seized evidence. I understand these items are located in a SCIF to which I do not have access.

the evidence I observed. My observations and findings rely on the credibility and reliability of the digital evidence provided to me by FBI employees, and of the procedures used to identify, collect, preserve, and examine that evidence.

III. Typical observations and findings

Due to the well-known and addictive nature of the child pornography (CP) industry, and crimes against children in general, certain observations and patterns of behavior are expected to emerge while investigating CP activity. In a CP investigation, for example, a digital forensic examiner such as myself typically would make the following observations about the digital evidence:

1. The CP material consists of many thousands of files, both photos and videos, organized by a hierarchy of directories with descriptive folder names.
2. A person logged in as the offending user took active steps to conceal the CP material.
3. CP material was accessed frequently, and on recent dates prior to the government's seizure of that material.
4. A variety of computer artifacts demonstrate attribution of CP activity to a particular user account.
5. If personal electronic communications are available, they demonstrate a consistent, frequent, and strong interest in and knowledge of CP material as information is shared among like-minded criminals.
6. There is a clear timeline, based upon other user activities (e.g., checking e-mail, logging into password-protected online accounts, etc.), identifying a particular person who was logged into the offending user account.

I have never examined digital evidence in a CP investigation where the above general observations were not made.

IV. Key Findings

A. Part One

The following findings are supported by my direct observations and examination of the digital evidence in this case.

1. Several photos and videos located on the seized digital evidence appear to be CP material.

Using Magnet AXIOM, a digital forensics application supplied by the FBI, I reviewed seized digital evidence that previously had been processed by FBI employees. I was able to confirm the existence of several hundred files consistent with the appearance of child pornography, including the four specific examples cited in the government's Complaint.

2. The CP material appears to have been intentionally concealed through the use of encryption.

I have reviewed several file listings related to the CP material. Each file listing is presumed to have been exported from a preserved data volume discovered on digital media seized by the government.

The first file listing, named "JAS_020240 [LinuxMintVM Directory Listing].csv" is a listing of all the files and folders discovered inside a virtual machine referred to as the "Linux Mint" VM.[2] The file listing indicates the encryption program Veracrypt was installed in the VM at the filesystem location:

```
mint-vg-root\NONAME [ext4]\[root]\usr\bin\veracrypt
```

In addition, it appears that a software package called eCryptfs (Enterprise Cryptographic Filesystem) was used to create an encrypted filesystem located at

```
mint-vg-root\NONAME [ext4]\[root]\home\.ecryptfs\josh\.Private\
```

Another file listing, named "JAS_020241 [JoshHomeDirectory Directory Listing].csv" provided a list of the contents of the encrypted filesystem, including a 54 gigabyte encrypted file named "data.bkp."

```
ecryptfs.yUQHr9ne\data.bkp
```

Decrypting this file revealed a container with hundreds of files appearing to be CP material. Its file listing, named "JAS_020242 [VeraCryptContainer Directory Listing].csv, included the four CP files cited in the government's Complaint.

It is noted that FBI employees were able to access the "Linux Mint" VM, the encrypted filesystem, the encrypted store "data.bkp," and even a second "data.bkp" file (not containing CP material) using the same shared passwords "gohan" and "gohan9740phi$".

3. The "Linux Mint" virtual machine (VM), containing the encrypted CP material, was discovered on Schulte's computer.

The file listing named "JAS_020238 [SC1 Directory Listing].csv" was generated from a volume called "Data" located on a hard drive attached to Schulte's computer seized by the FBI on

[2] A virtual machine (commonly referred to as a VM) is a computer system that runs inside of another computer system (For example, a Linux operating system running inside of a Windows operating system).

03/15/2017. According to this file listing, a folder named "Documents" contained a folder called "VMs," which contained a subfolder named "Linux Mint":

```
Data [NTFS]\[root]\Documents\VMs\Linux Mint\
```

Inside the Linux Mint folder were eight files consistent with supporting a virtual machine (VM). One of the files, "Linux Mint.vdi," is approximately 100 gigabytes in size is contains the memory, filesystem and data required to run the VM's "guest" operating system inside the Windows operating system. The .vdi extension suggests that this VM was created and accessed by a VM application called VirtualBox. The log files exported from this VM confirm this observation.

4. The existence of the "Linux Mint" VM on Schulte's computer was a result of a large, mass copy process of more than 200,000 files, transferred from another computer system on 05/06/2016.

I reviewed the file listing named "JAS_020238 [SC1 Directory Listing].csv" and observed that the \VMs\Linux Mint\ folder and all of its contents were copied as part of a large, continuous "mass copy" process that included more than 200,000 files and folders. By sorting the file listing by the Created date and noting the time differences between adjacent files in the listing, it is clear that the user had initiated a massive, logical copy of active files (i.e., files immediately available to the user) to the Documents folder located at:

```
Data [NTFS]\[root]\Documents\
```

The user initiated this file copy process at midnight, 05/06/2016, starting with the volume master file table ($MFT), which finished copying at 00:01:41 UTC. Thereafter, the remaining filesystem metadata files were copied, followed by files in the "Desktop" folder, then files in the "Documents" folder and its subfolders, followed by "Downloads," "Music," and other folders associated with a Windows user account. The files copied before and after the \VMs\Linux Mint\ folder contents were copied within a fraction of a second of those VM files, demonstrating that the user had no time to identify and single out those VM files for copying.

Indeed, the start time, copy order, and unbroken chain of Created timestamps is consistent with an automated copy task that had been scheduled and left unsupervised. I have observed no evidence that the user of Schulte's computer was even aware that the \VMs\Linux Mint\ folder was among the 200,000 items copied to his computer on 05/06/2016.

5. The "Linux Mint" VM was not accessed by any user of Schulte's computer.

After observing the \VMs\Linux Mint\ had been copied to the SC1 "Data" drive as part of a massive – likely automated – copy, I began to investigate when those files may have been accessed after they were copied.

One way to investigate whether files may have been accessed is by observing their filesystem Accessed dates. For all the files contained in the \VMs\Linux Mint\ folder, the last Accessed timestamps were identical to those of the Created dates (i.e., the dates they were copied[3]). However, since it is possible to turn off the ability for Windows to update Accessed times, I turned my attention to the Modified dates. I observed that the Modified dates for all the VM files *precede* their copy date, meaning none of the files, including the large "Linux Mint.vdi" file, had been modified after having been copied.

Since the slightest change to a file's data would necessarily update its filesystem Modified date, this observation means that the Linux Mint VM was never accessed at all – for more than ten months – between the date it was copied to Schulte's computer to the date it was discovered and seized by the FBI on 03/15/2017. My years of experience with CP investigations inform my opinion that this is not behavior indicative of a child pornographer.

6. No files contained inside the "Linux Mint" VM, including the CP material, were accessed or modified after 05/01/2016.

To determine whether the contents of the VM, including the encrypted CP material, had been accessed or modified inside the VM after it had been copied from its previous location, I analyzed the following file listings:

- JAS_020240 [LinuxMintVM Directory Listing].csv
- JAS_020241 [JoshHomeDirectory Directory Listing].csv
- JAS_020242 [VeraCryptContainer Directory Listing].csv

These listings contain the filesystem timestamps for the files in the VM, including those that had been observed in encrypted containers, such as the CP material. I did not observe any file or folder that had been created, accessed, or modified after 05/01/2016.

7. Schulte's computer was not technically capable of accessing the "Linux Mint" VM until the VirtualBox software was installed on 01/24/2017, more than eight months after the VM was copied.

The computer system to which the VM (and its encrypted CP material) were copied was not even capable of accessing a VM until 01/24/2017. This date corresponds to the installation date of the VirtualBox application, which I verified by examining the boot drive of Schulte's computer and analyzing a variety of Windows artifacts, including:

- Timestamps of the VirtualBox application files,

[3] When a file is copied from one filesystem to another, its Created date is changed to the date of the copy, because in effect the file is "recreated" or "reborn" in the new filesystem. However, the Modified date is preserved from the last time the file was modified on the previous filesystem.

- Prefetch files,
- Event logs, and
- Windows Registry files

None of the Windows artifacts I observed indicated that a VM-capable application was installed on Schulte's computer, using the current operating system, before 01/24/2017.[4] This observation means that no user, including Schulte, could have accessed any VM[5] prior to this date, which is more than eight months after the "Linux Mint" VM was copied. Again, this is not behavior indicative of a child pornographer.

8. The computer system from which the "Linux Mint" VM was copied had supported multiple user accounts.

Many computer systems belonging to Schulte were seized at the time of the FBI search on 03/15/2017. Some were in operation at the time of the search, and some were disconnected and stored in closets. It is likely certain previous systems had been wiped, reformatted, and "repurposed" prior to being stored.[6] For example, a tower labeled "B1" was found stored in a closet at the search scene and was later designated as "SC12" by the FBI.[7] According to its file listing "QNY20_SC12_RAID5_StoragePartition_HashList.csv," it had fewer than 200 active files, including filesystem "administrative overhead" metadata file. Most of this large volume was unallocated space, containing no active data, indicating this was likely a recycled/repurposed computer. If this was the original storage location of the "Linux Mint" VM, then the previous data is most likely lost.

That said, on 05/01/2016 data from this previous computer system was also copied to a "new" server, designated as "QNY56_SC48_SRV02," from which the FBI produced a file listing named "QNY56_SC48_SRV02_RAID_file_listing.csv," from one of its volumes. This copy process took place just days before the previously described mass copy of data to Schulte's

[4] In theory, applications such as VirtualBox could have been installed in a previously installed operating system, if the user chose to repurpose or upgrade the computer system.

[5] I discovered that the user had, in fact, created a single, Windows-based VM, using VirtualBox after it was installed. However, that VM (including its "Win.vdi" file) had been removed prior to the execution of the 03/15/2017 search warrant.

[6] During a 06/29/2017 interview, FBI agents reported Schulte's description of his rebuilding and repurposing of computer systems: "Each time he built a new computer, he wiped clean the computer he replaced and then repurposed it."

[7] In the same 06/29/2017 interview, Schulte was shown a photo of "1B20" and told the FBI agents, "1B20 had been giving him problems for a long time, certainly prior to [Schulte's] move to NYC. [Schulte] explained that he built 1B20 while he was employed at the CIA... [Schulte] advised that his old roommate, "Shavani," also used 1B20, as they 'played around with virtualization.'" It is likely this "1B20" computer is the same as the "QNY20" computer described by the referenced file listing.

desktop computer occurring on 05/06/2016. Unlike the copy event of 05/06/2016, however, it appears that the 05/01/2016 copying process occurred in at least three stages:[8]

- "backup" folders – 6:15:50 to 06:29:07 UTC
- "backup/pictures" – 15:09:20 to 15:13:32 UTC
- Other folders – 16:25:07 to 18:16:55 UTC

These actions resulted in the copying of nearly 100,000 files and folders, including **495 VMs**, from the previous computer system. According to the file listing of the destination computer, there were several users with account directories established in its home directory:

```
Partition 2\NONAME [ext4]\[root]\home\
```

These home directory names include "derek," "dschulte," "jack," "john," "josh," "kevin," "mdb," "Michael," "niall," "nort," "sturm," "timmy," and "tor." The /etc/passwd file exported from this Linux system confirms active user accounts corresponding to most of these directories, and also includes accounts for "root," and "irc."

Another computer system seized by the FBI was designated as "QNY56_SC48_SRV01," which had a volume represented by the file listing "qny56_sc48_srv01_raid_decrypted_file_listing.csv." This is another Linux system that appears to serve as storage for music, movies and TV shows. Under the \music\ directory I observed a directory for "cryptm_users."

```
NONAME [ext4]\[root]\music\cryptm_users\
```

This is likely a reference to the "cryptm.org" shared server cited six times in the government's Complaint as having been allegedly established to upload and store CP. I observed no files indicative of CP material in this volume. However, I did observe several subfolders in the "cryptm_users" folder that appear to correspond to user names, including "desol," "hpb," "john," "josh," "kevin," "niall," "nort," "nwg," "sturm," and "zoe." The government's Complaint cited an IRC chat quoting Schulte as telling his associates he had established user accounts for them, including "hpb" and "niall," to facilitate uploading their data, which the government claims is CP material. However, I only observed video files corresponding to published movies and TV shows stored in these user folders – not files indicative of CP material.

In fact, I have seen no evidence that CP material was ever uploaded to this server, or to the server cited in the Complaint. However, on 06/28/2009, less than ten minutes after the IRC conversation when the government alleges "SCHULTE appeared to discuss sharing an encrypted

[8] Copying processes, especially of "backup" folders, are often accomplished by using compression and packaging techniques that may preserve filesystem timestamps and thwart a complete understanding of the copying timeline.

server with other individuals to distribute child pornography," Schulte actually directs his associates to upload movies and TV shows into directories named "/movies" and "/shows." Those directories do appear in this same "qny56_sc48_srv01_raid" server seized by the FBI:

`NONAME [ext4]\[root]\movies\` – containing 1,138 video files of popular movies

`NONAME [ext4]\[root]\shows\` – containing 4,843 video files and folders, organized by folders for each TV show season

However, I did not observe any files in these folders that were indicative of CP material.

To summarize, Schulte established multiple shared servers including those storing several hundred VMs and commercially produced entertainment media. Moreover, the evidence suggests that Schulte provided broad access to his computer systems, enabling multiple users to create and store data as they pleased. There is no reason to doubt he provided this same broad access to multiple users on the now-defunct server from which he inadvertently copied the "Linux Mint" VM.

9. The computer system from which the "Linux Mint" VM was copied had contained multiple, identical VM "templates" apparently used for training and/or experimentation purposes.

As described earlier, it appears Schulte had created several hundred VMs on multiple shared servers. However, here I will limit my discussion to the 595 VMs stored on the volume designated as "QNY56_SC48_SRV02_RAID," because it appears that 495 of those VMs were copied from the malfunctioning server to this volume on 05/01/2016.

After analyzing the file listings named "QNY56_SC48_SRV02_RAID_file_listing.csv" and "QNY56_SC48_SRV02_RAID_Partition2_HashList.csv," I made the following observations regarding the 595 VMs:

- There appears to be a great variety of Linux-based and Windows-based VMs installed on the server.
- Most versions of VMs had a dozen or more "copies," based on the file names, folder names, and .vdmk[9] file sizes.
- Some copies of VMs were identical, even matching their hash values.[10]

[9] As the .vdi extension typifies a VM created by VirtualBox, the .vdmk extension typifies a VM created by VMware.

[10] Hashing is the process of applying a mathematical algorithm to a digital information that results in a fixed-length "fingerprint" of the hashed data. For example, if one bit of data is different between the content of two files then the hash values will be completely different.

- For most versions of VMs, there were some copies that were identical, and some that were not (hashes and file sizes did not match).[11]
- Some identical copies of VMs had different file names.

It is important to note that identical copies of VMs (those with matching hashes) have VM *content that is identical in every way*. They have the identical file system, operation system, user accounts, file permissions, and every other piece of data. These VM replicas are created from the same VM "template," so a user who opens one of these VMs will encounter the same environment, user account(s), and passwords as those of other replicas.

In these file listings I recognized some VM versions and copies as having been designed specifically for training purposes. These VMs are located in "SANS" directory:

```
Partition 2\NONAME [ext4]\[root]\home\josh\blackhat_laptop\Desktop\SANS\
```

I am confident these VMs are meant for training purposes because I earned eight of my cybersecurity certifications after taking courses from the SANS Institute, one of the leading cybersecurity training organizations in the world, and they make liberal use of VMs throughout their training programs. I also recognize VMs with the text "netwars-tournament" in their folder names because I personally competed in SANS Netwars tournaments multiple times.

In my expert opinion, there is no practical reason for a single user (such as Schulte) to create so many copies of so many versions of VMs for personal use. It is more likely these VM replicas were meant to be used by the many users of his computer system for the purpose of virtualization familiarity, training, and experimentation. The fact that all these VMs were stored in the "Josh" home directory means users of the VMs had read-write-execute privileges for files and folders in Josh's home directory and that any activity occurring there may not be directly attributable to Schulte. If hundreds of the VMs were copied from the now-defunct server that previously stored the "Linux Mint" VM, then any of the users on that previous system could have been responsible for creating the "Linux Mint" VM and storing their CP material there.

B. Part Two

The following findings are supported by my professional experience as well as my technical examination of evidence in this case.

1. The Google searches cited by the government's Complaint are not indicative of a history of searching for CP.

[11] For example, there seems to have been 31 copies of a VM named "Windows 8.1 x64-s0XX.vmdk," where XX is the copy number. Copies 1-5 and 16 have different hashes and larger file sizes, so likely they have been used and modified. However, copies 6-15 and 17-30 have identical hash values so they are exactly the same.

To support probable cause in the government's Complaint, the affiant presented several "Google searches" [12] whereby "SCHULTE appeared to search the Internet for child pornography." Here I have reproduced the examples they cited, and provided my response to each one.

"(i) on or about April 9, 2011, SCHULTE conducted a Google Search for "child pornography" on at least three occasions;"

Response: The government misinterpreted these Google records. It was a *single* search, with the user then viewing the image and video listings of the search results. No websites were visited as a result of this search. In online conversations with his friends (IRC chats), Schulte joked about searching Google for child pornography.

"(ii) on or about October 15, 2011, SCHULTE conducted Google Searches for "movie where father videos daughter and friend sex" and "movie where father videos child porn";"

Response: Noting the dates and times, these searches perfectly correspond to an IRC chat conversation about trying to remember the movie "Butterfly Effect." Obviously, the user was not searching for CP.

"(iii) on or about May 15, 2012, SCHULTE conducted a Google Search for "female teenage body by year.""

Response: The adjacent Google searches indicate the user was initially searching for "growth of human body by year," perhaps as an academic inquiry. Then after viewing multiple search results, he searched for "female human growth by year," then "growth," then "growth of female body" followed by a visit to an educational website about hormones, followed by more searches for "growth of female body," "growth of female body teenage years," and finally "female teenage body by year." In my experience, this behavior is not indicative of someone looking for CP.

At worst, the Google searches cited in the Complaint demonstrate a single search for "child pornography" among eleven (11) years of searches, and no web sites were visited as a result of that single search. Again, this is not behavior typical of a person with a strong disposition towards CP.

2. The IRC chat excerpts cited by the government's Complaint are not indicative of a person with a predisposition towards CP.

To support probable cause in the government's Complaint, the affiant presented five excerpts from Internet Relay Chat (IRC) conversations[13] whereby "SCHULTE and others appear to

[12] See Complaint, paragraph 6, p.12.

[13] See Complaint, paragraph 5, pp.7-12.

discuss, among other things, their receipt and distribution of child pornography." These five instances of alleged CP-related discussions were selected from four years of IRC chats, from 2009 to 2012. However, all selected chat excerpts were from 2009 – eight years prior to the 2017 search of Schulte's residence.

When attempting to use a person's words to characterize his predisposition towards a particular behavior, it is import to consider frequency and context of those expressed ideas. My observations about the IRC chats and the alleged instances of CP-related discussions are summarized below.

- **In IRC chats, each user is capable of changing his screen name at any time.** While it is possible that Schulte is responsible for the all the words written by someone using the screen name "josh," it is by no means assured. During these chats, users who entered the chat sessions as "guest" screen names frequently changed their names to "josh" (and vice-versa) and the user "josh" frequently changed his screen name to other names, such as "josh hates labs" and "josh_IBM." The phrase "is now known as" (indicative of a changed screen name) occurs 1065 times in the 2009 chats alone.[14]
- **Every IRC chat excerpt in the Complaint was taken out of the context of the larger conversation, thus obfuscating the true topic that was being discussed.** For example, in the last excerpt included in the Complaint, the user "sturm" (as is his custom) trolls "josh" by answering a question about the "cryptm" server that was being established. "Sturm" responds, "Josh started it so he could securely host all his child/rape porn." However, if one reads the IRC conversation for a few minutes before and after this joke was made, it is obvious the referenced server was being established to host video files of TV shows and movies, not CP. In fact, large folders named "shows" and "movies" containing video files (specifically mentioned later in this conversation) were found in a computer system seized by the FBI (see **Finding #8**). No CP material was found.
- **The excerpts in the Complaint frequently omit textual clues to joking.** For example, in the first excerpt in the complaint, the user "sturm" is attributed with the statement "A great place for kiddy porn!" followed by the "[….]" placeholder and then Schulte ("josh") saying "lol…" I noted the *only information* omitted by the "[….]" placeholder is the emoticon **;-p** (wink with tongue sticking out; being cheeky/playful). This emoticon[15] indicates the speaker was joking about his previous statement. There are many dozens of other examples of the Complaint omitting obvious clues to joking within and around the five alleged CP-related discussions in the IRC chats.

In my experience, a handful of mentions of and jokes about CP among friends, as cited in the Complaint, is not indicative of a typical child pornographer.

[14] The phrase "is now known as josh" occurs 137 times in the 2009 chats.
[15] See https://en.wikipedia.org/wiki/List_of_emoticons.

3. I found no definitive links to CP material on Schulte's computer system outside of the "Linux Mint" VM.

The government's Complaint alleges "some of the Websites known to contain child pornography appear to have been accessed by the user of the Desktop Computer." Here I note the allegation is that the user visited websites that *may contain* child pornography, not that any CP was searched for, downloaded, or even viewed by the user of Schulte's computer.

Using AD LAB, I processed the forensic image of the desktop computer and examined relevant temporary Internet files, browser history files, the WebcacheV01.dat file, the Index.dat file, and other files associated with software used to download data from the Internet. In my review of the relevant data, I discovered evidence of the user accessing several websites associated with adult pornography, such as xvideos.com and pornhub.com. In particular, I found several adult web site references in the WebcacheV01.dat file and in the \sitelogo\ folder of an installed program called "iTube Studio," which is used to download videos from online video streaming services.

While it is true that one or more of the visited adult web sites could potentially contain CP material, I have seen no evidence that CP material was actually downloaded to the Schulte computer from any of those web sites.

To be thorough, however, I conducted a global search for several text strings typically associated with CP content and CP file and folder names, such as "lolita," "kiddie," and "pthc" (preteen hardcore). The only substantive search "hits" I observed were found inside files associated with browser filters (designed to prevent the viewing of CP), and a handful of instances within several chat logs with unknown participants.

V. Conclusion

According to the government's allegations, Schulte knowingly received, possessed, and transported the CP material that was found in an encrypted container, hidden inside a VM that was stored on his computer. However, after an extensive forensic analysis of the digital evidence, I see no indication that Schulte knew that a hidden, containerized, group of CP files were among the 200,000 files he had copied on May 6, 2016. Further, I see no indication that he had accessed, or even attempted to access, the VM containing the CP files after the mass copy. Based on my understanding of his background and experience, Schulte certainly would have known how to create and access VMs.

The fact that Schulte did not single out the Linux Mint VM files for copying, but rather included them in a mass copy process of 200,000 files demonstrates that the copying of CP material was most likely inadvertent. The fact that Schulte chose not to access the Linux Mint VM – at any time during the 10+ months it was stored on his server – demonstrates that he had no interest in its contents, if in fact he even realized it was there.

The fact that Linux Mint VM files were copied from a shared server to which many people had user accounts, as well as (very likely) unfettered access and broad permissions[16], demonstrates that in fact the CP could have been downloaded, encrypted, and stored by any user of that unsecured server. The presence of hundreds of VM "templates" is further evidence of the presence of multiple users of that system.

The Google searches and IRC excerpts cited in the Complaint do not support the characterization of Schulte having a history of engaging with CP material. The Google searches were largely misinterpreted and did not consider other user behavior adjacent in time. A complete and accurate reading of IRC conversations reveal that participants are in a perpetual state of joking around, demonstrating only a passing curiosity about child pornography topics.

While it is impossible to prove a negative (e.g., that a crime has not been committed), I have observed no evidence in this case directly linking Schulte's behavior to the knowing receipt, possession, and transportation of CP material.

It is my expert opinion that the VM containing CP material, having been created by any of dozens of users of a shared computer system, was inadvertently copied to Schulte's computer, where it remained neither viewed nor accessed for many months until its eventual discovery by the government.

I reserve the right to change or update my opinions on this matter as new information is provided to me.

Respectfully Submitted,

J. Richard Kiper, PhD, PMP
FBI Special Agent (Retired) and Forensic Examiner

[16] Multiple IRC conversations indicate the user "josh" had a very casual and unsecure approach to passwords and permissions when establishing his shared servers.